DATA BREACH

POLICY

Last Updated: 10/03/2019

Contents

Data Breach Process

Although REACH takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving REACH

However the breach has occurred, the following steps should be taken immediately:

1. Internal Notification:

Individual who has identified the breach has occurred must notify the Data Protection Officer (DPO). A record of the breach should be created using the following templates:

a. Data Breach Incident Form (Appendix A)
b. Data Breach Log (Appendix B)
c. Evidence Log (Appendix C)

2. Containment:

DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. Recovery:

DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up electronic records to restore lost or damaged data)

4. Assess the risks:

Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification Form (Appendix A):

a. What type of data is involved
b. How sensitive is it?
c. If data has been lost/stolen, are there any protections in place such as encryption?
d. What has happened to the data?
e. What could the data tell a third party about the individual?
f. How many individuals data have been affected by the breach?
g. Whose data has been breached?
h. What harm can come to those individuals?
i. Are there wider consequences to consider such as reputational loss?

5. Notification to the Information Commissioner's Office (ICO):

Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification Form (Appendix A) can be completed and emailed to casework@ico.org.uk.

6. Notification to the Individual:

The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by REACH.

7. Evaluation:

The DPO should assess whether any changes need to be made to REACH processes and procedures to ensure that a similar breach does not occur.

Appendix A

Data Breach Notification Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	
Whose data has been breached:	
What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss:	

Part C: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	

Appendix B

Data Breach Log

Date Reported:	Notified By:	Reported To:	Description of Breach:	Notification to ICO:	Notification to Individual(s)	Further Actions to be taken:	Reviewed by:
				Yes/No	Yes/No		
				Yes/No	Yes/No		
				Yes/No	Yes/No		

Appendix C

Data Breach: Evidence Log

Date:	Description of Evidence:	Details of where evidence is stored/located:	Member of staff who collected data: